REMARKS

Applicant thanks the Examiner for the thorough consideration given the present application. Claims 1-20 are currently being prosecuted. The Examiner is respectfully requested to reconsider his rejections in view of the remarks as set forth below.

Rejection under 35 U.S.C. 103

Claims 1-20 stand rejected under 35 U.S.C. 103 as being obvious over Ji et al. (US Patent 6,392,872) in view of Hsiao et al. (US Patent 6,496,944). This rejection is respectfully traversed.

First, applicants wish to clarify which references are being applied in the rejection. The Examiner identifies the primary reference as Ji et al. and gives the patent number 6,392,872. However, this patent number does not include Ji as an inventor. It is assumed that the Examiner meant to refer to US Patent 5,889,943 which was used in a previous action. If this is incorrect, the Examiner is requested to clarify which reference is being applied.

The Examiner states that Ji substantially teaches the invention, and in particular teaches a backup/recovery system for protecting a computer system including an application layer, a detecting module where the detecting module retrieves predetermined data in order to determine whether there is an executable file. The Examiner admits that Ji does not teach creating a module which

2

creates a restore point prior to downloaded predetermined data arrival. However, the Examiner states that Ji does show a capability of detection and elimination of electronic mail virus including a connectivity among clients/servers, virus or error detected transmitted between sources and destination and data transferred from one area to another.

The Examiner relies on Hsiao to teach a system for backup/recovery computer system including data restoration and reconstruction of the file system to any previous file system state. The Examiner feels it would have been obvious to one of ordinary skill in the art to apply the data restoration and reconstruction of the file system to any previous file system state as taught by Hsiao in conjunction with the apparatus and method as taught by Ji. The Examiner feels that this modification would have been obvious, and one skilled in the art would have been motivated to provide the error or virus detection and correction within a backup/recovery management computer system environment for the instant computer system performance and processing in order to provide continuity network operating system functionality.

Applicant disagrees that this combination of references teaches the present claimed invention. Ji provides an apparatus for detecting and eliminating viruses which may be introduced by messages sent through a postal node of a network electronic mail system includes polling and retrieval modules in communication with

3

the postal node to determine the presence of unscanned messages and to download data associated with them to a node for treatment by a virus analysis and treatment module. A method for detecting and eliminating viruses introduced by an electronic mail system includes polling the postal node for unscanned messages, downloading the messages into a memory of a node, and performing virus detection and analysis at the node.

However, Hsiao provides a database management system (DBMS) which is used to maintain a record of a file system's directory structure (registry database). The creation, removal or update of a directory results in a record, pertaining to that event, being stored into a database table of similar events. In addition, files are also linked to a DBMS (user database) and archived according to its management rules (i.e. DBMS references and/or controls the linked files). In the event of a file system crash, the DBMSs are used to restore the file system through the use of the directory structure database table which allows reconstruction of the file system to any previous file system state. Furthermore, files can then be recovered to match that state and thereby reconcile external files linked to a database to any previous state. See Col. 2, lines 35-48.

Thus, Ji provides Internet real-time virus detection. Apparently, it appears that a virus treatment module treats messages found to contain a virus. Accordingly, the database

4

management system provided by Hsiao would be redundant to the apparatus taught by Ji.

The claims of the present invention describe a backup/recovery system for protecting a computer system. A system in accordance with the present invention comprises a detecting module, located within said computer system, for monitoring a predetermined data; a creating module, located within said computer system, for creating a restore point; wherein said detecting module retrieves said predetermined data, in order to determine whether there is an executable file contained therein for judging said backup/recovery system to backup data in said computer system or not, said creating module creates a restore point prior to downloading said predetermined data, which contains said executable file, said interface implements a predetermined procedure thereafter and said application layer involves accessing said predetermined data and said backup/recovery system enables restoring said computer system to a previous state which is prior to said downloaded predetermined data arrival.

Applicant submits that the references of record do not teach or suggest the limitations of the claims of the present invention.

In particular, the references do not teach or suggest the limitation of the detecting module judging the backup/recovering system to the backup data in the computer system, and the creating

5

module of creating a restore point prior to downloading the predetermined data.

In a situation involving an undefined virus, Hsiao may be used to restore the file system through the use of a directory structure database table which allows reconstruction of the file system to a previous file system state. However, Hsiao does not take into consideration the backup operation prior to making changes to the data in the computer system. As a result, Hsiao fails to restore the computer system to a previous state which is exactly equivalent to the operational state of the computer system prior to the downloaded predetermined data arrival. Thus, such a system does not properly maintain the data for the user.

This differs from the present invention which establishes recovery points for storing data in the computer system by backing up the prior data on the hard disk beforehand. The conventional recovery techniques of a file system directory structure described by Hsiao does not overcome the problem of the loss of data in the computer system, nor does Ji teach or suggest the limitation of creating a restored point prior to downloading the predetermined data which contains the executable file as recited in the present claims. Accordingly, neither Ji nor Hsiao nor any combination of the references renders obvious the claims of the present application. Accordingly, Applicant submits that this rejection is overcome.

In view of the above remarks, it is believed that the claims clearly distinguish over the patents relied upon by the Examiner, either alone or in combination. In view of this, reconsideration of the rejections and allowance of all of the claims are respectfully requested.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Robert F. Gnuse (Reg. No. 27,295) at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By_____
    Joe McKinney Muncy, #32,334

KM/RFG:gmh
3667-0102P

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000